

REMARKS

The objection to claim 11 has been obviated by the amendment to claim 11 to remove the clause "connected to the firewall device and".

The Examiner has rejected claims 1,2 and 7-11 under 35 USC 102(e) as anticipated by US patent 6,453,353 to Win et al, and claims 5-6 have been rejected under 35 USC 103 as obvious from US patent 6,453,353 to Win et al. Claim 3 has been rejected as obvious over the combination of Win and Ramachandran, U.S. 5,978,850. Claim 3 has been rejected as obvious over the combination of Win and Ramachandran, U.S. 5,978,850 and in further view of Gillies et al., U.S. 6,253,211.

In response to the prior art rejection, claims 1 and 10 have been cancelled and the dependent claims have been amended to depend from new claim 11 which was added in the amendment filed 7/6/05. New claim 11 is directed to a firewall having a wireless communication device connected to it.

A notice of appeal has been filed with this response in case this response is not sufficient to place the case in condition for allowance.

In response to the first office action, and the applicant's response to it, the Examiner issued a final rejection. The Examiner stated in response to arguments of the applicant (at pp. 6-7 of the final rejection) that a recitation of the intended use of the claimed invention must result in a structural difference between the claimed invention and the prior art in order for the claim to patentably distinguish from the prior art.

The Examiner's reasons for rejecting applicant's previously made arguments is not understood since there is a clear structural distinction between the Win patent and original claims 1 and 10 and now independent claim 11. Both original claims 1 and 10 and new claim 11 recite a limited management user interface wireless device which can conduct a limited

number of management operations from the full management system over a wireless remote connection.

The Win patent does not teach such a limited management interface device that allows a limited set of management functions to be conducted wirelessly in addition to a full management interface implemented at the location of the network to be managed. Win only discloses a full management interface, namely an administrative application incorporated in an administrator work station 700 shown in Figure 7. The only mention anywhere in the Win patent of the word “wireless” is the following passage from the discussion of Figure 9 at Col. 26, lines 29-43:

Computer system 900 also includes a communication interface 918 coupled to bus 902. Communication interface 918 provides a two-way data communication coupling to a network link 920 that is connected to a local network 922. For example, communication interface 918 may be an integrated services digital network (ISDN) card or a modem to provide a data communication connection to a corresponding type of telephone line. As another example, communication interface 918 may be a local area network (LAN) card to provide a data communication connection to a compatible LAN. **Wireless links may also be implemented.** In any such implementation, communication interface 918 sends and receives electrical, electromagnetic or optical signals that carry digital data streams representing various types of information.

A fair reading of this passage is that the computer 900 running the management application may be wirelessly connected to the local network 922 and internet 928 in Figure 9. But nowhere is there mention of both a full management interface and a limited management interface coupled wirelessly so that a limited set of management commands can be issued from the wireless device.

The Win patent goes on to teach that the administration application 114 can delegate administration of user, roles, servers or system to other administrations by defining an administration role to specific users. When the administration role is assigned to a user, that user has a right to perform administration functions. Such a delegated role to a user is not the same thing as the limited management user interface element of the claimed invention.

The reason this is true is the correct interpretation of the claim element in claim 11. The pertinent language of claim 11 is:

for conducting a limited number of management operations of the full management system for the network security application

(emphasis mine)

The following passage from page 1, line 5 of the specification at bar tells us what the "network security application" is that is being managed:

The invention relates in general to network security. In particular the invention relates to managing a network security application, such as a firewall, security gateway, Intrusion Detection System (IDS) or Virtual Private Network (VPN) gateway.

Thus, the limited management device connected wirelessly has the capability to perform a limited set of management functions on firewalls, security gateways, Intrusion Detection Systems or Virtual Private Network Gateways or the like.

In contrast, the following passages from Win (part of which were cited by the Examiner) detail the limited management functions that may be performed by the delegated administrative roles taught by Win:

In many contexts, centralized administration of a system is undesirable. To overcome this problem, Administration Application 114 can delegate administration of users, roles, servers or the system to other administrators. The system 2 defines a special type of role, called an Admin Role. When the Admin Role is assigned to a user, that user has the right to perform administrative functions.

An example of an Admin Role is "Help Desk Administrator." An enterprise might have a dozen such administrators located at various sites of the enterprise.

Each Admin Role is defined by an Administrative Role ID value, an Administrative Role Name, a Functional Group value, a Description, an Administrative Privilege, and a Server Configuration value.

The Administrative Role ID value uniquely identifies the Admin Role. The Administrative Role Name value is the name of the Admin Role that is displayed to users and administrators working with the Admin Role. The Functional Group value identifies one of the functional groups that is associated with the Admin Role. Each Admin Role may be assigned to only one functional group.

In one embodiment, the Administrative Privilege value has one of the four exemplary values set forth in Table 1, which describes the administrative functions that can be carried out by each of the privilege levels. The Server Configuration value indicates whether this Admin Role can modify server configuration information.

TABLE 1
ADMINISTRATIVE FUNCTIONS
ADMINISTRATION PRIVILEGE LEVEL

	Help	Role	User		
FUNCTION	Desk	Admin	Admin	System	
find, view a user record	YES	YES	YES	YES	
reset user's password	YES	NO	YES	YES	
view user's roles	YES	YES	YES	YES	

assign, remove particular NO	YES	YES	YES
roles from user records			
create, delete, modify user NO	NO	YES	YES
records			
all administrative functions NO	NO	NO	YES
except those defined by the			
configuration privilege			

None of these delegable functions involves management of firewalls, security gateways, Intrusion Detection Systems or Virtual Private Network Gateways or the like. Properly interpreted, Win does not teach the same invention as independent claim 11 or any of its dependent claims because it does not teach both a full management device and a wireless limited management device which can manage firewalls, security gateways, Intrusion Detection Systems or Virtual Private Network Gateways or the like.

Further, the Examiner stated that claim 11 is anticipated because Win's system includes one or more firewalls. (Col. 21, lines 50-58). This is not the same invention. In Win, Figure 8 discloses firewalls 802 and 804 arranged to protect the access server. Win fails to teach that a firewall is provided with a network security application, a full management user interface which comprises mechanisms for conducting management operations for the network security application over a secure data connection, and a wireless communication device configured to provide a limited management user interface for conducting a limited number of management operations of the full management system for the network security application over a wireless remote connection. On the contrary, no mention of management for the firewall device is made in Win. Win relates only to management of access of user to the access server 106 and not to management of firewalls, security gateways, Intrusion Detection Systems or Virtual Private Network Gateways or the like.

Furthermore, the Win patent does not address the same problem as is addressed by the claimed invention and so the Win solution is not the same invention as the claimed invention. That problem is stated in the following passages from page 3, line 13 et seq.

Typically the management user interface and a central management system are in a fixed computer or work station connected to an internal network (or a plurality of such computers or work stations) and the connection between the management user interface and the network security applications is a fixed connection. The reason for this is security (accessing the management system only from a physically secure location) and the fact that the management application is a complex application and running it for example over a conventional modem connection

might be very slow. On the other hand, this means that this fixed computer or work station needs to be physically accessed in order to manage the managed applications. Thus, in order to react to information provided by the network security applications the management user interface needs to be monitored. The management system is commonly arranged to generate an alarm message, for example on a computer screen of a management user interface, as a response to predetermined (suspicious/malicious) actions or failures and therefore the output of the network security applications does not need to be analysed constantly. However, finding and fixing the conditions causing the alarm to go off requires human intervention, and therefore the alarms generated by the network security applications need to be monitored, by system administrators.

The network security applications are commonly arranged to send alarms for example to a predetermined pager device or as an SMS (Short Message Service) message to a predetermined mobile phone. Such pager device or mobile phone is typically carried with some administrator of the network security applications in order to receive the alarms instantly without somebody having to sit by the management user interface at all times. However, the alarm is only a short message indicating that something is wrong and the administrator receiving the alarm may not be even close to the management system or user interface, and therefore processing the alarm still needs the administrator to get to the management user interface in order to find out the reason for the alarm and to fix the situation.

It would be beneficial for the administrator to be able to fix the problem right away when receiving the alarm and therefore to be able to manage the network security applications in a more flexible manner and to respond to failures more rapidly.

Therefore, the problem the invention solves is in networks that have full management interfaces to provide a wirelessly connected limited management interface device with limited capability to send some management commands so that a network can be fixed immediately when an alarm is sent to the wireless device. This precludes the necessity of having somebody manning the full management console at all times to keep the network running trouble free. The invention is to have both a full network management interface and a limited management interface device connected wirelessly so network managers can fix problems immediately as they occur so long as the problem can be fixed by the limited set of management functions available through the wireless management device.

This problem is not addressed in the Win reference. The following passages from

Win Col. 1, line 66 et seq illustrate the problem Win solved and the needs his invention addressed:

One approach to some of the foregoing problems and needs has been to provide each network resource or application program with a separate access control list. When a user connects to the network, the user is presented with a listing of available applications. The user selects an application for use or execution. The access control list identifies users or hosts that are authorized to access a particular application. As new users or hosts are added to the network, the access control lists grow, making security management more complicated and difficult. Use of a large number of separate lists also makes the user experience tedious and unsatisfactory.

Another disadvantage of the foregoing approaches is duplication of management processes. To add new users to the system, a network administrator must repeat similar access processes for each application or resource to be made available to the new users. The redundancy of these processes, combined with rapid growth in the number of users, can make the cost of deploying, managing and supporting a system unacceptably high.

Thus, there is a need for a mechanism to govern access to one or more information resources in which selective access is given to particular users.

There is also a need for such a mechanism that is equally adaptable to an internal network environment and to an external network environment.

There is a further need for such a mechanism that is easy to configure and re-configure as new users and resources become part of the system.

There is still another need for such a mechanism that is simple to administer.

There is a need for such a mechanism that blocks access to, or does not display to the user, those applications for which the user does not have access rights.

There is a need for such a mechanism that is integrated with a flexible, adaptable, additive data model that permits rapid and convenient addition of information describing users and resources, and that automatically propagates the effects of changes in the data model throughout the system.

Note that Win does not address the problem of remote management of a network wirelessly using a wireless limited management functionality device in addition to a full management interface device. Because he does not address this problem, his solution does not include both a full management interface and a wireless management interface device.

For anticipation to exist, all the elements of the claim must appear in the allegedly anticipating reference, arranged as in the claim. Lindemann maschinenfabrik GmbH v. Amercan Hoist & Derrick Co., 730 F.2d 1452 (Fed. Cir. 1984). In short, the reference must

teach the same invention. For the Examiner to make out a prima facie case, the Examiner must interpret each element of the claim according to the claim language itself and the teachings of the specification and then point out where each element is found in the anticipating reference and point out how the elements of the claim are in the reference united in the same way.

This the Examiner has not done. There is no teaching of both a full management interface plus a limited management interface device coupled wirelessly to the network to be managed.

Claim 11 has as its elements:

- a network security application,
- a full management user interface which comprises mechanisms for conducting management operations for the network security application over a secure data connection, and
- a wireless communication device ~~connected to the firewall device and~~ configured to provide a limited management user interface for conducting a limited number of management operations of the full management system for the network security application over a wireless remote connection.

To make out a prima facie case of anticipation, the Examiner was supposed to point where the Win reference teaches “a wireless communication device configured to provide a limited management user interface for conducting a limited number of management operations”.

The passage cited by the Examiner, Col. 26, lines 29 to 39 does not teach both a wireless limited management user interface device and a full management user interface device with the wireless device provided so that error messages sent to the wireless device can be corrected immediately from the wireless device. This passage only teaches that the full management interface can be connected to the network wirelessly. This is not the same invention.

The Obviousness Rejections

PATENT

Obviousness cannot be established by combining the teachings of the prior art to produce the claimed invention absent some teaching, suggestion or incentive to do so. In re Bond, 910 F.2d 831, 834, 15 USPQ2d 1566, 1568 (Fed. Cir. 1990). Suggestion arises from one of ordinary skill in the art perceiving a likelihood of success in solving the problem the inventors solved by making the combination. In other words, the consistent criterion for determination of obviousness is whether the prior art would have suggested to one of ordinary skill in the art that this process should be carried out *and would have a reasonable likelihood of success, viewed in the light of the prior art*. See Burlington Industries v. Quigg, 822 F.2d 1581, 1583, 3 USPQ2d 1436, 1438 (Fed.Cir.1987); In re Hedges, 783 F.2d 1038, 1041, 228 USPQ 685, 687 (Fed.Cir.1986).

Suggestion either arises or does not arise based upon the totality of the circumstances. The totality of the circumstances includes the problem addressed by the invention, the advantages, characteristics or properties it has etc. as well as all the other factors identified herein.

Here, the Win patent is not directed to the same problem, and the combination of Win and the other references does not have the same properties as the claimed invention. This is because any combination of the prior art references does not have a limited management wireless device which has the capability to manage firewalls, security gateways, intrusion detection systems, etc.

One of the big questions in deciding on the existence or non existence of obviousness is was all the knowledge needed to make the claimed invention present in the prior art. Where the prior art of a combination of references cited in support of an obviousness rejection does not teach an element needed to solve the problem the claimed invention solved, the obviousness argument must fail. In re Hayes Microcomputer Products, Inc., 982 F.2d 1527, 1541, 25 USPQ2d 1241 (Fed. Cir. 1992) [failure of prior art to teach a

claimed method of detecting escape sequences in modems doomed obviousness invalidity argument of infringer even though escape sequences themselves were admittedly in the prior art].

Here, the prior art combinations (all of them) are lacking an element of knowledge needed to make the invention: a limited management wireless device capable of managing firewalls, security gateways etc. Where the combination of prior art is lacking a key element of the claims, it is not fair to say that the prior art combination suggests the claimed invention.

Another big question with regard to whether suggestion exists is were the elements combined in the claimed combination used in the prior art for the same purpose or do the same work as they do in the claimed combination? Here, the answer is no. The limited management interface that is described in the Win patent is not used for the same purpose and does not do the same work as the limited management wireless device in the claimed invention. This is because the Win limited management interface is not taught to manage firewalls, security gateways etc.

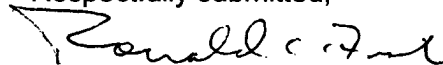
Because of the factors identified above, one skilled in the art would not perceive a likelihood of success in solving the problem the invention solved by combining the teachings of

PATENT

the three prior art references cited by the Examiner. Accordingly, suggestion does not exist, and the obviousness rejection must fail.

Enclosed are two U.S. patent publications corresponding to the PCT publications WO 0127787 and WO 0069120 (U.S. 2002061599 and 2004181690, respectively) the Examiner stated he did not consider in the Information Disclosure Statement filed 6/15/05.

Respectfully submitted,



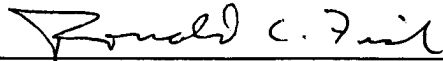
Ronald Craig Fish
Reg. No. 28,843
Tel 408 778 3624
FAX 408 776 0426

Dated: January 9, 2006

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail, postage prepaid, in an envelope addressed to: Commissioner for Patents, Mail Stop Amendment, P.O. Box 1450, Alexandria, Va. 22313-1450.

on

1/9/06
(Date of Deposit)



Ronald Craig Fish, President
Ronald Craig Fish, a Law Corporation
Reg. No. 28,843